

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*A White Apple iPhone with IMEI number 357341096271181,
containing SIM card number 89148000005673596268

Case No. 1:21-mj-520

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

18 U.S.C. 922

Possession by a Prohibited Person

The application is based on these facts:

Please See Attached Affidavit

☒ Continued on the attached sheet.


☐ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Brandon Stahlhut, SA, ATF

Printed name and title

Sworn to before me and signed in my presence.
via FaceTime video

Date: Jul 2, 2021City and state: Cincinnati, Ohio
Karen L. Litkovitz
United States Magistrate Judge

ATTACHMENT A

The device to be searched:

White Apple iPhone,

IMEI Number: 357341096271181, containing SIM card number 89148000005673596268

The device is currently located in the ATF Evidence Room at 550 Main Street, Cincinnati, Ohio, Room 8-491.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

The following items/information that may be located on and in the Device described in Attachment A which would be material evidence to show a violation of 18 U.S.C. § 922(g)(1) by Carlito RILEY from July 2020 through the present:

1. Data that may identify the owner or user of the above-described cellular communication device(s);
2. Address books and calendars;
3. Audio and video clips related to the above-described criminal activity and further described in this affidavit in support of the search warrant, for the above-described item(s);
4. Call histories and call logs related to the above-described criminal activity and further described in this affidavit in support of the search warrant, for the above-described item(s);
5. Photographs and associated metadata¹ related to the above-described criminal activity and further described in this affidavit in support of the search warrant, for the above-described item(s);
6. Text messages (SMS²), multimedia messages (MMS³), recorded messages and subscriber information modules [SIM cards⁴] between Carlito RILEY and any co-conspirators involved in the criminal activity as described in the Affidavit in support of the search warrant, for the above described item(s);

¹Metadata is generally defined as data about data. It is stored within the data file itself, but is not normally seen when viewing the file. Metadata includes Exchangeable Image File Format (EXIF) which is a specification for image file formats used by digital camera and includes specific information about the photograph.

²Short Message Service (SMS) is the text communication service that allows the exchange of short text messages between mobile phone devices.

³Multimedia Message Service (MMS) is a communication service that allows the exchange of messages that include multimedia content to and from mobile phones.

⁴Subscriber Identity Modules, sometimes referred to as SIM cards, are portable memory chips often used in notebook computers and some models of mobile phones. SIM cards securely store the service-subscriber key used to identify subscribers. The SIM card allows users to change phones by simply removing the SIM card from one mobile phone and inserting it into another mobile phone or broadband telephony device. SIM cards store information used to authenticate and identify subscribers, including but not limited to the Service Provider Name, Service Dialing Numbers and Value Added Service applications. They can also be used to store personal address books and SMS data.

7. E-mail messages and attachments, whether read or unread, and related to the above-described criminal activity and further described in this affidavit in support of the search warrant, for the above-described item(s)
8. Internet World Wide Web (WWW) browser files including, but not limited to, browser history, browser cache, stored cookies; browser favorites, auto-complete form history and stored passwords;
9. Global position system (GPS⁵) data including, but not limited to coordinates, way points and tracks;
10. Documents and other text-based files related to the above described statutes related to criminal activity, and as further described in the Affidavit in support of the search warrant.

⁵The Global Positioning System (GPS) is a satellite-based navigation system which provides location and time information.

**IN THE UNITED STATES DISTRICT COURT
FOR SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION**

**IN THE MATTER OF THE SEARCH OF A
CELLULAR TELEPHONE DESCRIBED
AS:**

CASE NO. 1:21-mj-520

A White Apple iPhone with IMEI number
357341096271181, containing SIM card
number 89148000005673596268

**LOCATED AT THE ATF EVIDENCE
ROOM, 08-491 FEDERAL BUILDING, 550
MAIN STREET, CINCINNATI, OHIO 45202**

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Brandon Stahlhut, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an

electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment A.

2. I am a Special Agent (SA) with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and have been so employed since February 2019. As a part of my training with the ATF, I graduated from the Federal Law Enforcement Training Center, Criminal Investigator Training Program, located in Glynco, Georgia. I also graduated from the ATF Special Agent Basic Training Academy, located in Glynco, Georgia. In my career with the ATF, I have been assigned to the Cincinnati Field Office in the Southern Judicial District of Ohio. Prior to my employment with ATF, I was a member of the United States Secret Service in Washington, D.C. where I served as a member of the Uniformed Division under the Presidential Protective Division. I was employed in that capacity from April 14, 2009, to February 4, 2019. I am also a graduate of Northern Kentucky University, where I received a bachelor's degree in Political Science in 2007.

3. This affidavit is submitted in support of an application for a federal search warrant for the following device as there is probable cause to believe that evidence of a crime—namely, violations of 18 U.S.C. § 922(g)(1) – Possession by a Prohibited Person, exists therein. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is:

- A White Apple iPhone with IMEI number 357341096271181, containing SIM card number 89148000005673596268

hereinafter referred to as the “Device.” The Device is currently located at the ATF Cincinnati Field Office, located at 8-491 Federal Building, 550 Main Street, Cincinnati, Ohio 45202.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On July 4, 2020, at approximately 2120 hours, officers with the Cincinnati Police Department (CPD) were dispatched to the area of 1701 Kinney Avenue for a report of a shooting. Upon arrival, officers located a crime scene and recovered over 30 shell casings in the street at the location. Officers interviewed several witnesses who advised that at least two individuals had been struck by gunfire, but officers were unable to locate any victims at the scene. Shortly thereafter, another CPD officer advised that two individuals had arrived at the University of Cincinnati Medical Center (UCMC) Emergency Room in separate vehicles and both individuals were suffering from gunshot wounds. Both vehicles used to transport these victims were held as crime scenes.

7. A CPD detective responded to UCMC and learned that one of the victims was Kiontaye Riley, who had been taken into emergency surgery with life threatening gunshot wounds. The detective learned that Kiontaye Riley was driven to the hospital by Carlito RILEY (no relation to Kiontaye Riley) in a 2018 grey Hyundai Tucson bearing Ohio license plate GVU1314, one of the vehicles held as a crime scene.

8. Carlito RILEY gave the detective consent to search his vehicle. During the search, officers located a loaded Glock, model 23, .40 caliber pistol, bearing serial number ZDH129 located under the rear portion of the passenger side front seat. Officers observed blood evidence on the Glock as well as a bullet hole in the area where the slide and the frame came together.

This bullet hole had rendered the firearm inoperable. Several pieces and a spring belonging to the pistol were found on the rear passenger side floorboard. Officers also located a loaded Taurus, Model PT111 G2, 9mm pistol bearing serial number TKR67539 from under the front driver's seat.

9. The detective verbally advised Carlito RILEY of his Miranda Rights, and executed a written notification of rights which Carlito RILEY signed before conducting a taped interview. During the interview Carlito RILEY denied any knowledge or possession of the Glock, Model 23 pistol that was recovered under the front passenger seat. Carlito RILEY did confess to possessing the Taurus, Model PT111 G2, pistol that was recovered under the front driver's seat. Carlito RILEY admitted to knowing he was prohibited from possessing a firearm due to a prior criminal conviction for drug trafficking.

10. Prior to July 4, 2020 Carlito RILEY had been convicted of a crime punishable by a term of imprisonment exceeding one year. Specifically, Carlito RILEY was convicted in the Hamilton County (Ohio) Court of Common Pleas of aggravated trafficking in drugs (F3) and having weapons while under disability (F3) in case number B1806166.

11. As part of the investigation, an interstate nexus expert examined both of the recovered firearms. The nexus expert determined that the Taurus, Model PT111 G2, 9mm pistol bearing serial number TKR67539 is a firearm as defined in Title 18, United States Code, Chapter 44, Section 921(a)(3) and the firearm was manufactured outside the state of Ohio and therefore traveled in interstate and/or foreign commerce prior to July 4, 2020.

12. All the events described above occurred within the Southern District of Ohio.

13. On May 13, 2021, the Honorable Stephanie K. Bowman, United States Magistrate Judge for the Southern District of Ohio, signed a criminal complaint against Carlito RILEY in

case number 1:21-MJ-00418 for a violation of 18 U.S.C. § 922(g) based on the above facts. An arrest warrant was issued for Carlito RILEY on the same date.

14. On June 3, 2021, Carlito RILEY approached security personnel at the Federal Building at 550 Main St, Cincinnati OH, 45202, and attempted to turn himself in. CPD was contacted and officers responded and took Carlito RILEY into custody. CPD transported Carlito RILEY to the Hamilton County Justice Center (HCJC), 900 Sycamore St, Cincinnati, OH, where he was held pending state charges. At the time of his arrest Carlito RILEY had on his person one white Apple iPhone, bearing IMEI 357341096271181 (the Device). The Device was stored with Carlito RILEY'S personal property at the HCJC.

15. On June 7, 2021, your affiant and another special agent transported Carlito RILEY to Federal Court and transferred Carlito RILEY into United States Marshals custody for his initial appearance. At this time, your affiant took possession of the Device and transported it to the ATF Cincinnati Field office, 550 Main St, Cincinnati OH, where is currently being held.

16. Your affiant knows based upon his training and experience in investigating firearms violations and firearms trafficking, that individuals routinely use their cell phones in furtherance of their firearm possession. Specifically, firearm possessors and traffickers often discuss business arrangements via text message, email, social media, and other means of communication. These individuals also often photograph themselves with firearms. These photographs are then stored and maintained on their cell phones. Their cell phones also often contain information about conspirators, including contact information, call logs, and text messages.

17. Based upon the aforementioned facts and circumstances, your affiant believes that the cell phone and SIM card recovered during the course of the investigation will contain

evidence of Carlito RILEY'S illegal possession of firearms, 18 U.S.C. § 922(g)(1) – Possession by a Prohibited Person.

18. The Device is currently in the lawful possession of the ATF and is currently in storage at the ATF, located at 8-491 Federal Building, 550 Main Street, Cincinnati, Ohio 45202. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of law enforcement.

19. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence of a crime, namely Title 18 U.S.C. § 922(g)(1) – Possession by a Prohibited Person – exists and can be found within the white Apple iPhone, bearing IMEI 357341096271181 containing SIM card number 89148000005673596268, which is currently located at the ATF, 8-491 Federal Building, 550 Main Street, Cincinnati, Ohio 45202.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing

names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media includes various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to

store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer

software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, which is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

21. Based on my training, experience, and research, I know that the Device has capabilities that allows it to serve as **“a wireless telephone, digital camera, portable media player, GPS navigation device, PDA and Tablet.”** In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

23. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contains electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

24. *Forensic evidence.* As further described in Attachment A, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crime described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device

consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* Because this warrant seeks only permission to examine a Device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

27. Based on the above facts and circumstances, your affiant believes that Carlito RILEY did possess a firearm illegally, in violation of Title 18 U.S.C. § 922 (g)(1). I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device, described as a white Apple iPhone with IMEI number 357341096271181 containing SIM card number 8914800005673596268 which was possessed by Carlito RILEY to seek the items described in Attachment A.

REQUEST FOR SEALING

28. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them

publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Further affiant sayeth naught.



Brandon Stahlhut
Special Agent, ATF
Cincinnati, OH

Subscribed and sworn to me this 2nd day of July, 2021.



Karen L. Litkovitz
United States Magistrate Judge



ATTACHMENT A

The device to be searched:

White Apple iPhone,

IMEI Number: 357341096271181, containing SIM card number 89148000005673596268

The device is currently located in the ATF Evidence Room at 550 Main Street, Cincinnati, Ohio, Room 8-491.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

The following items/information that may be located on and in the Device described in Attachment A which would be material evidence to show a violation of 18 U.S.C. § 922(g)(1) by Carlito RILEY from July 2020 through the present:

1. Data that may identify the owner or user of the above-described cellular communication device(s);
2. Address books and calendars;
3. Audio and video clips related to the above-described criminal activity and further described in this affidavit in support of the search warrant, for the above-described item(s);
4. Call histories and call logs related to the above-described criminal activity and further described in this affidavit in support of the search warrant, for the above-described item(s);
5. Photographs and associated metadata¹ related to the above-described criminal activity and further described in this affidavit in support of the search warrant, for the above-described item(s);
6. Text messages (SMS²), multimedia messages (MMS³), recorded messages and subscriber information modules [SIM cards⁴] between Carlito RILEY and any co-conspirators involved in the criminal activity as described in the Affidavit in support of the search warrant, for the above described item(s);

¹Metadata is generally defined as data about data. It is stored within the data file itself, but is not normally seen when viewing the file. Metadata includes Exchangeable Image File Format (EXIF) which is a specification for image file formats used by digital camera and includes specific information about the photograph.

²Short Message Service (SMS) is the text communication service that allows the exchange of short text messages between mobile phone devices.

³Multimedia Message Service (MMS) is a communication service that allows the exchange of messages that include multimedia content to and from mobile phones.

⁴Subscriber Identity Modules, sometimes referred to as SIM cards, are portable memory chips often used in notebook computers and some models of mobile phones. SIM cards securely store the service-subscriber key used to identify subscribers. The SIM card allows users to change phones by simply removing the SIM card from one mobile phone and inserting it into another mobile phone or broadband telephony device. SIM cards store information used to authenticate and identify subscribers, including but not limited to the Service Provider Name, Service Dialing Numbers and Value Added Service applications. They can also be used to store personal address books and SMS data.

7. E-mail messages and attachments, whether read or unread, and related to the above-described criminal activity and further described in this affidavit in support of the search warrant, for the above-described item(s)
8. Internet World Wide Web (WWW) browser files including, but not limited to, browser history, browser cache, stored cookies; browser favorites, auto-complete form history and stored passwords;
9. Global position system (GPS⁵) data including, but not limited to coordinates, way points and tracks;
10. Documents and other text-based files related to the above described statutes related to criminal activity, and as further described in the Affidavit in support of the search warrant.

⁵The Global Positioning System (GPS) is a satellite-based navigation system which provides location and time information.